

IN THE CLAIMS

Please make the following claim substitutions:

1 1. (Currently amended) A method for use in a system which includes a
2 cryptographic key store for storing a transformed cryptographic key and
3 accessing circuitry for accessing the transformed cryptographic key from the
4 cryptographic key store, the method comprising the step of:

5 storing key re-transforming information for the transformed cryptographic
6 key in a decryption store, the accessing circuitry being able to communicate with
7 the decryption store exclusively via a predetermined interface, the interface being
8 such that the accessing circuitry is unable to access from the decryption store at
9 least one of: a) at least a portion of the key re-transforming information, and b) at
10 least a portion of the cryptographic key;

11 wherein said key re-transforming information has a transformation pattern
12 randomly generated by said decryption store.

1 2. (Original) The method of claim 1 wherein the interface is such that the
2 accessing circuitry is unable to access from the decryption store both of: a) at
3 least a portion of the key re-transforming information, and b) at least a portion of
4 the cryptographic key.

1 3. (Currently amended) The method of claim 1 wherein the key re-
2 transforming information further comprises [[:]]
3 ~~a transformation pattern; and~~
4 a key decrypting algorithm.

1 4. (Original) The method of claim 3 wherein the transformation pattern
2 comprises a unique identifier of the decryption store.

1 5. (Original) The method of claim 1 further comprising the steps of:
2 the decryption store receiving the cryptographic key;
3 the decryption store transforming the cryptographic key using key
4 transforming information to produce the transformed cryptographic key; and

5 the decryption store sending the transformed cryptographic key to the
6 cryptographic key store.

1 6. (Original) The method of claim 1 wherein:
2 the decryption store comprises a mobile terminal;
3 the cryptographic key store comprises a computer memory; and
4 the accessing circuitry comprises a processor.

1 7. (Original) The method of claim 1 wherein:
2 the decryption store comprises a network access card;
3 the cryptographic key store comprises a computer memory; and
4 the accessing circuitry comprises a processor.

1 8. (Original) The method of claim 1 further comprising the steps of:
2 the decryption store receiving the transformed cryptographic key and
3 information;
4 the decryption store re-transforming the transformed cryptographic key
5 using the key re-transforming information to produce the cryptographic key; and
6 the decryption store encrypting the information using the cryptographic
7 key to produce encrypted information.

1 9. (Original) The method of claim 8 further comprising the step of
2 transmitting the encrypted information.

1 10. (Original) The method of claim 1 further comprising the steps of:
2 the decryption store receiving encrypted information;
3 the decryption store receiving the transformed cryptographic key;
4 the decryption store re-transforming the transformed cryptographic key
5 using key re-transforming information to produce the cryptographic key; and
6 the decryption store decrypting the encrypted information using the
7 cryptographic key to produce decrypted information.

1 11. (Original) The method of claim 10 further comprising the step of the
2 accessing circuitry accessing the decrypted information.

1 12. (Original) The method of claim 1 wherein the accessing circuitry's
2 communication with the decryption store comprises the transfer of information
3 between them.

1 13. (Original) The method of claim 1 wherein the storing step comprises
2 storing the transformed cryptographic key in the cryptographic key store for a
3 period of time.

1 14. (Original) The method of claim 1 further comprising the step of erasing
2 the cryptographic key from the decryption store at the completion of each
3 cryptographic operation.

1 15. (Original) The method of claim 1 wherein the cryptographic key is
2 stored in the decryption store in such a way that it disappears from the decryption
3 store when the decryption store is removed from the system.

1 16. (Currently amended) A system comprising:
2 a cryptographic key store for storing a transformed cryptographic key;
3 a decryption store for storing key re-transforming information for the
4 transformed cryptographic key, the decryption store having a predetermined
5 interface;
6 accessing circuitry coupled to the cryptographic key store, the accessing
7 circuitry being able to access the transformed cryptographic key in the
8 cryptographic key store, and to communicate with the decryption store
9 exclusively via the predetermined interface, the interface being such that the
10 accessing circuitry is unable to access from the decryption store at least one of:
11 a) at least a portion of the key re-transforming information, and b) at least a
12 portion of the cryptographic key;
13 wherein said key re-transforming information has a transformation pattern
14 randomly generated by said decryption store.

1 17. (Currently amended) The ~~method~~ system of claim 16 wherein
2 interface is such that the accessing circuitry is unable to access from the

3 decryption store both of: a) at least a portion of the key re-transforming
4 information, and b) at least a portion of the cryptographic key.

1 18. (Original) The system of claim 16 wherein:
2 the decryption store comprises a mobile terminal;
3 the cryptographic key store comprises a computer memory; and
4 the accessing circuitry comprises a processor.

1 19. (Original) The system of claim 16 wherein:
2 the decryption store comprises a network access card;
3 the cryptographic key store comprises a computer memory; and
4 the accessing circuitry comprises a processor.

1 20. (Original) The system of claim 16 wherein the decryption store further
2 comprises:
3 an input port for receiving the transformed cryptographic key;
4 a key decrypting module for decrypting the transformed cryptographic key
5 using the key re-transforming information to produce the cryptographic key;
6 an encrypting module for encrypting information using the cryptographic
7 key to produce encrypted information.

1 21. (Original) The system of claim 20 wherein the decryption store further
2 comprises a transmitter for transmitting the encrypted information.

1 22. (Original) The system of claim 16 wherein the decryption store further
2 comprises:
3 an input port for receiving the transformed cryptographic key;
4 a key decrypting module for decrypting the transformed cryptographic key
5 using the key re-transforming information to produce the cryptographic key;
6 a decrypting module for decrypting encrypted information.

1 23. (Original) The system of claim 22 wherein the decryption store further
2 comprises a receiver for receiving the encrypted information.

1 24. (Original) The system of claim 16 wherein the decryption store further
2 comprises:

3 a receiver for receiving the cryptographic key;
4 a key encrypting module for encrypting the cryptographic key using key
5 transforming information to produce the transformed cryptographic key; and
6 an output port for outputting the transformed cryptographic key.

1 25. (Currently amended) A decryption store for storing key re-
2 transforming information for a transformed cryptographic key, the decryption
3 store comprising:

4 a predetermined interface, the interface being operable to receive the
5 transformed cryptographic key; and

6 an output port complying exclusively with the predetermined interface
7 such that information is accessible from the decryption store through the output
8 port;

9 wherein at least one of: a) at least a portion of the key re-transforming
10 information, and b) at least a portion of the cryptographic key being not
11 accessible from the decryption store through the output port; and

12 wherein said key re-transforming information has a transformation pattern
13 randomly generated by said decryption store.

1 26. (Currently amended) The ~~method~~ invention of claim 25 wherein
2 interface is such that at least both of: a) at least a portion of the key re-
3 transforming information, and b) at least a portion of the cryptographic key are
4 not accessible from the decryption store through the output port.

1 27. (Original) The invention of claim 25 wherein the decryption store
2 comprises a mobile terminal.

1 28. (Original) The invention of claim 25 wherein the decryption store
2 comprises a network access card.

1 29. (Original) The invention of claim 25 wherein the decryption store
2 further comprises:

3 a key decrypting module for decrypting the transformed cryptographic key
4 using the key re-transforming information to produce the cryptographic key;

5 an encrypting module for encrypting information using the cryptographic
6 key to produce encrypted information; and

7 a decrypting module for decrypting encrypted information.

1 30. (Original) The invention of claim 29 wherein the decryption store
2 further comprises a transmitter for transmitting the encrypted information.

1 31. (Original) The invention of claim 25 wherein the decryption store
2 further comprises:

3 a receiver for receiving the cryptographic key;

4 a key encrypting module for encrypting the cryptographic key using key
5 transforming information to produce the transformed cryptographic key.

1 32. (Original) The invention of claim 31 wherein the transformed
2 cryptographic key is a function of a transformation pattern.

1 33. (Currently amended) The ~~method~~ invention of claim 32 wherein the
2 transformation pattern comprises a unique identifier of the decryption store.

1 34. (Currently amended) A method for use in a decryption store having
2 a predetermined interface and an output port complying exclusively with the
3 interface such that information is accessible from the decryption store through
4 the output port and at least one of: a) at least a portion of the key re-transforming
5 information, and b) at least a portion of the cryptographic key, is not accessible
6 from the decryption store through the output port, the method comprising the step
7 of:

8 storing key re-transforming information for a transformed cryptographic
9 key in the decryption store;

10 receiving the transformed cryptographic key; and

11 decrypting the transformed cryptographic key to produce the cryptographic
12 key;
13 wherein said key re-transforming information has a transformation pattern
14 randomly generated by said decryption store.

1 35. (Original) The method of claim 34 wherein the interface is such that at
2 least both of: a) at least a portion of the key re-transforming information, and b) at
3 least a portion of the cryptographic key are not accessible from the decryption
4 store through the output port.

1 36. (Currently amended) The method of claim 34 wherein the key re-
2 transforming information comprises [[:]]
3 ~~a transformation pattern; and~~
4 a key decrypting algorithm.

1 37. (Original) The method of claim 36 wherein the transformation pattern
2 comprises a unique identifier of the decryption store.

1 38. (Original) The method of claim 34 further comprising the steps of:
2 the decryption store receiving the cryptographic key;
3 the decryption store transforming the cryptographic key using key
4 transforming information to produce the transformed cryptographic key; and
5 the decryption store sending the transformed cryptographic key to a
6 cryptographic key store via the output port.

1 39. (Original) The method of claim 34 wherein the decryption store
2 comprises a mobile terminal.

1 40. (Original) The method of claim 34 wherein the decryption store
2 comprises a network access card.

1 41. (Original) The method of claim 34 further comprising the steps of:
2 the decryption store receiving information; and

3 the decryption store encrypting the information using the cryptographic
4 key to produce encrypted information.

1 42. (Original) The method of claim 41 further comprising the step of
2 transmitting the encrypted information.

1 43. (Original) The method of claim 34 further comprising the steps of:
2 the decryption store receiving encrypted information; and
3 the decryption store decrypting the information using the cryptographic
4 key to produce decrypted information.

1 44. (Original) The method of claim 43 further comprising the step of
2 sending the decrypted information to accessing circuitry via the output port.